CLAIMS

We claim:

✓1. A method for testing security of a cryptography device performing a cryptographic algorithm, comprising the steps of:

a. generating a faulty computation in the cryptography device;

b. receiving the faulty computation in a processor; and

c. using the faulty computation, the processor determining heretofore secret information stored in the cryptography device.

2. The method of claim 1, wherein the faulty computation is intentionally generated.

3. The method of claim 2, wherein the faulty computation is intentionally generated by subjecting the cryptography device to a physical stress.

4. The method of claim 3, wherein the step of subjecting the cryptography device to physical stress further includes subjecting the cryptography device to at least one of radiation, an atypical voltage level, and a higher clock speed than the cryptography device was designed to accommodate.

5. The method of claim 1, further comprising the step of transmitting the faulty computation from the cryptography device to a second cryptography device housing the processor.

6. The method of claim 1, wherein the cryptographic algorithm generates a digital signature which may be separated into linear components, wherein the step of determining heretofore secret information further comprises the processor comparing an erroneous signature having the generated fault on a digital message with a correct digital signature on the same digital message.

7. The method of claim 1, wherein the faulty computation is generated by inverting at least one bit stored in a register of the cryptography device.

8. The method of claim 7, wherein the step of determining heretofore secret information further comprises the processor comparing a correct value and an erroneous value containing the induced fault to determine the secret information.

9. The method of claim 1, wherein the cryptographic algorithm generates a digital signature, wherein the method further comprises the steps of:

a. the step of generating a faulty computation further comprises inducing a faulty computation in a plurality of digital messages; and

b. the step of determining heretofore secret information further comprises:

(i) the processor using a first fault to determine heretofore secret information;

(ii) the processor constructing sets of data for the cryptography device;

(iii) the processor receiving from the cryptography device responses to the sets of data; and

(iv) the processor using the heretofore secret information and the responses to determine a secret key.

10. The method of claim 1, wherein the cryptographic algorithm is an authentication algorithm, wherein:

a. the step of receiving the faulty computation comprises receiving the faulty computation in response to a challenge; and

b. the step of determining heretofore secret information further comprises the processor using the faulty computation to determine a single bit of heretofore secret information; and

c. repeating steps (a) and (b) above to determine a plurality of bits of secret information.

/ 11. A method for testing the security of a cryptography device which performs a cryptographic algorithm which generates a digital signature which may be separated into linear components, the method comprising the steps of:

a. storing in a memory a correct digital signature E for a message m generated by the cryptography device;

b. storing in the memory an incorrect digital signature $\hat{E}$ for the message m generated by the cryptography device; and

c. using E and $\hat{E}$, a processor determining heretofore secret information.

12. The method of claim 11, wherein method is performed by the processor, the method further comprising the steps of:

a. the cryptography device sending E to the processor; and

b. the step of determining heretofore secret information further comprises the first processor determining heretofore secret, information stored in the cryptography device.

13. The method of claim 11, wherein the step of determining heretofore secret information further comprises the processor determining secret information q stored in the cryptography device using:

$$\gcd(E-\hat{E}, N) = q$$

wherein N is a product of prime numbers, and one of the prime numbers is q.

14. A method for testing the security of a cryptography device performing cryptographic authentication algorithm, the method comprising the steps of:

a. receiving from the cryptography device a value $r^2 \bmod N$, wherein r is a random number and N is a secret value which is a product of prime numbers;

b. generating a subset of integers S and providing the subset S to the cryptography device;

c. receiving from the cryptography device $\hat{y} = (r + \acute{E})\Pi_{i \in s} s_i$ in response to the subset S, wherein $\hat{y}$ is an erroneous value, s_i is a secret exponent used to encrypt, and $\acute{E}$ is a value added to r due to an error;

d. a processor determining a value of $\acute{E}$ by computing:

$$(r+\acute{E})^2 = \frac{\hat{y}^2}{\Pi_{i \in s} v_i} \pmod{N}$$

wherein $v_i = s_i^2$

e. the processor determining a value of r by computing:

$$(r+\acute{E})^2 - r^2 = 2\acute{E}r + \acute{E}^2 \pmod{N}$$

and

f. using the values of $\acute{E}$ and r, the processor determining s_i by computing:

$$\prod_{i \in s} s_i = \frac{\hat{y}}{r+\acute{E}} \pmod{N}.$$

~~15. The method of claim 14, wherein the step of determining s_i further includes the step of the cryptography device computing:~~

$$\prod_{i\in S} s_i = \frac{2\acute{E}\hat{y}}{\frac{\hat{y}^2}{\prod_{i\in S} v_i} - r^2 + \acute{E}^2} \text{ (mod } N) .$$

~~16. The method of claim 14, further comprising the step of verifying whether the value of $\acute{E}$ is correct.~~

~~17. The method of claim 16, wherein the step of verifying further includes the step of using the subset S to determine whether the value of $\acute{E}$ satisfies the relation $(y')^2 = (r')^2 T^2$;~~

~~wherein T is a guessed value for $\Pi_{i\epsilon s} s_i$~~

~~18. The method of claim 14, further comprising the steps of:~~

~~a. the processor generating a plurality of subsets S;~~

~~b. the processor receiving a value in response to each subset S; and~~

~~c. using known values and the response value to each subset S, the processor determining heretofore secret information.~~

~~19. The method of claim 18, wherein the step of generating the plurality of subsets S further comprises generating singleton sets.~~

~~20. A method for testing the security of a cryptography device performing a cryptographic authentication algorithm by determining secret information comprising a number of bits, the method comprising the steps of:~~

~~a. a processor obtaining an erroneous digital signature $\hat{E}$;~~

~~b. the processor selecting a block length;~~

~~c. the processor determining a candidate vector w that matches all known bits of the secret information and is zero everywhere else;~~

~~d. the processor determining if the candidate vector w is correct;~~

~~e. if the candidate vector w is correct, the processor outputting a value for the selected block length; and~~

~~f. if the candidate vector w is incorrect, the processor determining another candidate vector.~~

~~21. The method of claim 20, wherein steps (c) - (f) are performed for a plurality of block lengths.~~

~~22. The method of claim 20, wherein the step of determining the candidate vector w further comprises determining:~~

$$w=\sum_{y=k_i}^{n} s_j 2^j + \sum_{j=k_i-r}^{k_i-1} u_j 2^j.$$

~~wherein k_i is a time at which an error may have occurred; s_j is a bit which may be incorrect; r is a possible blocklength; and u is a bit which may be incorrect.~~

23. The method of claim 20, wherein the step of determining if the candidate vector w is correct further comprises determining:

$$\exists e \epsilon \{0, \ldots, n\} \quad s.t. \quad (\hat{E}_j \pm 2^e m_j^W)^{ei} = m_j \pmod{N}$$

wherein e = a public exponent;

n = a number of bits in the secret information;

m_j = is a message;

e_i = is a public signature verification exponent; and

N = a product of prime numbers.

24. A method for testing the security of a first cryptography device performing cryptographic authentication algorithm by using a second cryptography device to determine secret information comprising a number of bits stored in the first cryptography device, the method comprising the steps of:

a. the second cryptography device sending to the first cryptography device a challenge t;

b. the first cryptography device receiving t and generating a response $u = r + ts$ mod p, wherein:

r is a random number selected by the first cryptography device;

s is the first cryptography device's secret key; and

p is a large prime number;

c. the second cryptography device receiving u;

d. the first cryptography device receiving t again and generating a response $\hat{u} = \hat{r} + x$ mod p, wherein:

$\hat{r}$ is an erroneous value of *r* and *x* is *t*s mod *p*; and

e. the second cryptography device receiving $\hat{0}$ and determining a location of the error.

25. The method of claim 24, wherein the step of determining the location of the error further comprises the steps of trying all possible locations of the error.

26. The method of claim 25, wherein the step of trying all possible locations further includes the step of determining which location for the error satisfies:

$$g^{\hat{0}} = g^{2i}\ g^{r} g^{X} \pmod{p}$$

wherein:

g is a generator of Z^*_p ; and

i is a location of the error.

27. A cryptography device produced according to the steps of:

a. generating a faulty computation in the cryptography device;

b. receiving the faulty computation in a processor; and

c. using the faulty computation, verifying that the processor cannot determine secret information stored in the cryptography device.

28. The device of claim 27, further comprising providing the cryptography device before generating the faulty computation.

29. The device of claim 27, wherein the faulty computation is intentionally generated during testing of the cryptography device.

30. The device of claim 29, wherein the faulty computation is intentionally generated during testing of the cryptography device by subjecting the cryptography device to a physical stress.

3,1. The device of claim 29, wherein the step of subjecting the cryptography device to physical stress further includes subjecting the cryptography device to at least one of radiation, an atypical voltage level, and a higher clock speed than the cryptography device was designed to operate on.

32. The device of claim 27, wherein the cryptography device performs a cryptographic algorithm which generates a digital signature which may be separated into linear components, wherein the step of verifying that the processor cannot determine secret information further comprises the processor verifying that an erroneous digital signature having the generated fault on a digital message cannot be compared with a correct signature on the same digital message.

33. The device of claim 27, wherein the faulty computation is generated by inverting at least one bit stored in a register of the cryptography device.

~~34. The device of claim 33, wherein the step of verifying that the processor cannot determine heretofore secret information further comprises verifying that the processor cannot compare a correct value and an erroneous value containing the induced fault to determine the secret information.~~

~~35. A cryptography device that is impervious to a hardware fault-based attack, which attack comprises the steps of:~~

~~a. generating a faulty computation in the cryptography device;~~

~~b. receiving the faulty computation in a processor; and~~

~~c. using the faulty computation, the processor determining secret information stored in the cryptography device.~~

~~36. The device of claim 35, further comprising providing the cryptography device before generating the faulty computation.~~

~~37. The device of claim 35, wherein the faulty computation is intentionally generated during testing of the cryptography device.~~

~~38. The device of claim 37, wherein the faulty computation is intentionally generated during testing of the cryptography device by subjecting the cryptography device to a physical stress.~~

39. ~~The device of claim 38, wherein the step of subjecting the cryptography device to physical stress further includes subjecting the cryptographic device to at least one of radiation, an atypical voltage level, and a higher clock speed than the cryptography device was designed to operate on.~~

ADD A27